







Bureau of Mines Information Circular/1982

Reliability of Computerized Mine-Monitoring Systems

By Raymond M. Kacmar



UNITED STATES DEPARTMENT OF THE INTERIOR

Information Circular 8882

Reliability of Computerized Mine-Monitoring Systems

By Raymond M. Kacmar



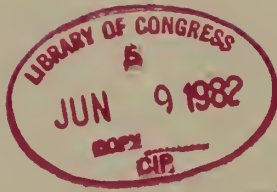
UNITED STATES DEPARTMENT OF THE INTERIOR

James G. Watt, Secretary

BUREAU OF MINES

Robert C. Horton, Director

TN295
24
no. 8882



This publication has been cataloged as follows:

Kacmar, Raymond M

Reliability of computerized mine-monitoring systems.

(Information circular ; 8882)

Supt. of Docs. no.: I 28.27:8882.

1. Mine safety--Data processing. 2. Mine gases--Data processing.
3. Mine fires--Data processing. 4. Reliability (Engineering). I. United States. Bureau of Mines. II. Title. III. Series: Information circular (United States. Bureau of Mines) ; 8882.

~~TN295-U4~~ 622s [622'.8'02854] 82-600074 AACR2

CONTENTS

	<u>Page</u>
Abstract.....	1
Introduction.....	2
Advantages and limitations of monitoring systems.....	3
Need for reliable systems.....	4
Definition of reliability terms.....	4
Reliability research program.....	8
Conclusion.....	10

ILLUSTRATION

1. Failure rate as function of equipment age.....	6
---	---

RELIABILITY OF COMPUTERIZED MINE-MONITORING SYSTEMS

By Raymond M. Kacmar¹

ABSTRACT

This paper describes the Bureau of Mines research program on the reliability of computerized mine-monitoring systems. The basic concepts of computerized monitoring are introduced along with its advantages and limitations. Current Bureau projects covering mine-monitoring systems are described, and some of the major areas of concern that should be addressed by future projects are outlined.

¹Electrical engineer, Pittsburgh Research Center, Bureau of Mines, Pittsburgh, Pa.

INTRODUCTION

Federal regulations (Code of Federal Regulations, Title 30, Part 75) require the environmental monitoring of the atmosphere of underground mines for methane, oxygen deficiency, carbon dioxide, air quantity, and indications of incipient fires. Conventionally, this monitoring is done with stain tubes, flame safety lamps, machine-mounted devices, thermal detectors, and various portable instruments. Except for machine-mounted methane monitors, which are operative only while the machines are powered, and thermal detectors along beltways, this monitoring is intermittent and may not give adequate indications of the conditions between instrument readings. What is needed to improve this situation is a mine-monitoring system that operates continuously and reliably so that unsafe conditions can be detected and dealt with promptly.

Current systems that are being marketed to fill this need can be generally categorized as computerized mine-monitoring systems. The hardware components of this type of system basically consist of transducers that monitor various parameters in the mine and associated components that process the data obtained. The number of transducers and the amount of processing performed vary from system to system according to the manufacturer and also the complexity of the mine in which the system is installed. The transducers most commonly used for environmental monitoring measure one or more of the following parameters: Methane, coal dust, carbon monoxide, airflow, temperature, relative humidity, differential pressure between airways, oxygen, noise, smoke, hydrogen sulfide, and submicrometer particulates.

In addition to these, transducers can be deployed for gathering production management data, providing equipment maintenance supervision, inventory control, event recording, and numerous other management reporting and documentation purposes.

Data from all the transducers previously discussed must be converted to engineering units, checked and processed to determine the status of conditions in the mine, and then displayed as needed.

The equipment normally required to perform this function consists of one or more computers and the associated peripherals and input-output interfaces. In the basic system the output from a transducer is converted to a format that enables a signal to be transmitted to a central computer station. There, a processor (or system of processors) tabulates the data, compares it with preset alarm conditions, displays results, logs the data for future reference, and performs other calculations and data management.

It is also possible to expand the system. This can be done by using a concept known as distributed processing. In this type of system, computing power is distributed by adding other noncentralized processing stations in the mine, thereby reducing the computational load on the central station. As an example, a processing station could be located adjacent to a group of transducers. This local station would be able to process the data and display results, alarms, or other information as needed. It would then send these data to the central station only as requested, allowing the central station to perform more system management operations.

For a computer system to operate, however, it must be programmed. Software modules must be written for each of the functions the system must perform, and an operating system must be developed that will combine these modules with the hardware to provide a working unit. Some of the main software modules inherent to monitoring systems follows: Initialize, read transducer data, test alarm limits, respond to keyboard commands, control peripherals, and manage communication system.

These modules can be written either in the assembly language for the individual processors used or in a high-level language, which can offer more versatility.

To complete the system, a transmission scheme must be defined. Two generic types of technology that are currently in use are the tube bundle and

telemetry approaches. The tube bundle system aspirates gas samples to analyzers at a central location, usually on the surface. The telemetry system places transducers near the actual mine conditions to be monitored, and the data obtained are then encoded and transmitted to a central location either on the surface or underground.

ADVANTAGES AND LIMITATIONS OF MONITORING SYSTEMS

The tube bundle system has some desirable features and has been used where response times were not critical and high-accuracy instruments were desired to detect small changes in gas concentrations. Because the instruments, pumps, and valving can be located external to the mine, they are easily accessible for maintenance, repair, and calibration. This allows the system to be independent of the underground mine power. Additionally, since the equipment can be located in fresh air, there are no problems with permissibility in coal mines. However, several limitations make this system not generally useful for multipurpose environmental monitoring; for instance, the system cannot be used for monitoring relative humidity, certain absorptive gases, or the operating status of various kinds of equipment. Its primary usage has been for spontaneous combustion and fire detection monitoring.

Telemetry systems are useful when a large number of points are to be monitored, fast response is required, and distances are large. The underground configuration usually has outstations located in fresh air connected to the common communications line and powered from the distribution system. The outstations contain power supplies which are hardwired to power remote transducers located in the intake airways. If the transducers are located in the returns or face areas, the power supplies and transducers must be permissible, usually utilizing intrinsically safe technology. This reliance on mine power seriously compromises system integrity from both a reliability and a functional usefulness

point of view. Mine power is notorious for its wide fluctuations in voltage level and for the presence of very large and unpredictable transients which lead to early equipment failure or cause equipment malfunctions. Also, mine power is turned off routinely on both a scheduled and an unscheduled basis, rendering the system inoperable. Sometimes this may be when the system can provide its greatest benefits, such as when the mine is unmanned.

The main advantages of a computerized mine-monitoring system (either tube bundle or telemetry) derive from the continuous nature of the data received from the system. These data show the output of the various transducers at any particular time of interest and are continuously reported, providing indications of the levels of oxygen, carbon monoxide, methane, airflow, and other mine conditions as needed. Diagnostic data can be recorded; for example, fan speed and pressure can be monitored, providing advance warning of fan failures. Advantages also include the easy storage and retrieval of the data and the availability of the data at a central location with the possibility of adding additional readout units wherever necessary.

An item of concern when installing a computerized mine-monitoring system measuring environmental parameters would be the location of the transducers. To provide complete and accurate coverage of an area of interest, several transducers may be required. In the face area, these modules would necessarily be located in high-traffic areas and would therefore

have to be moved frequently. Also, because of the way current regulations are written, these systems would not be able to replace a certified person making the measurement and, therefore, would at present only provide additional data as far as complying with the regulations was concerned.

In some applications, however, where certain operating conditions prohibit the

development of extra entries, continuous monitoring of carbon monoxide levels along the beltway could enable the operator to petition the Mine Safety and Health Administration (MSHA) for a variance to enable the beltway to be used as a fresh air intake. This would be possible because of the data obtained from a continuous-monitoring system.

NEED FOR RELIABLE SYSTEMS

The environmental parameters that are being dealt with in underground computerized monitoring all have a serious and immediate impact on life safety in the mine. By necessity then, monitoring systems must have a high degree of operational integrity to provide the protection for which they are intended.

The need for having a reliable system can be demonstrated in two approaches, safety and cost. In regard to safety, for a computerized mine-monitoring system the potential for three basic failure modes exists: Failing to give an alarm, giving a false alarm, and providing inaccurate data. The first failure mode gives the operator a false sense of security by implying that all conditions in the mine are safe, when in reality, a potentially unsafe condition exists. The second type of failure mode, false alarms, can cause problems by initiating remedial action that is not necessary. Repeated false alarms also erode confidence in the monitoring system. This reduced confidence can result in indecisiveness during real emergencies, with the possible result of the

operator simply turning off the alarm with the attitude of "it's just another false alarm, why bother to check it out." The third failure mode, inaccurate data, is included in addition to the other failures because of the continuous nature of the data received from the mine-monitoring system. These continuous data can be plotted and then compared with past data. When inaccurate information can be unknowingly recorded, it makes the decision of whether current trends are normal or unsafe less dependable.

With regard to cost, the operator gets major benefits from reduced costs in the following areas: There is more feedback on production activities (for example, by knowing in advance that an unsafe condition is forming, the operator can make corrective changes before a problem arises that would force the shutting down of equipment); service and maintenance costs of the system are reduced; less inventory is needed to maintain the system; and acceptance by the mining personnel reduces malfunctions related to user dissatisfaction.

DEFINITION OF RELIABILITY TERMS

For a computerized mine-monitoring system to be accepted by the mining industry and to be used to its fullest potential, it must be demonstrated that it can provide the proper data and that this information can then be used to make

logical decisions about the conditions in the mine. The data received from a computerized mine-monitoring system can only be meaningful, however, if the method of obtaining the data is reliable.

Using a formal definition, reliability is the probability the system will perform its intended functions during a specified time interval, under stated conditions. Reliability planning, therefore, has to account for the environment the equipment will be subjected to and also reflect the amount of time during which the equipment will be operated.

For reliability analysis, there are three basic failure categories, as shown in figure 1:²

Early failures (infant mortality) - where the failure is due to manufacturing defects that were undetected by quality control checks. Decreasing failure rate.

Chance failures (random failures) - where a system that has not failed is as good as new and, hence, its failure behavior during any period of service depends only on the length of that period and not on the system's past history. Constant failure rate.

Wear-out failures - where a system fails owing to the wearing out of components. Increasing failure rate.

The useful life of a system, then, can be defined as the period of time after infant mortality and before equipment components wear out.

Early failures occur during the initial phases of an equipment's life and are normally the result of substandard materials being used or a malfunction in

the manufacturing process. When these mistakes are not caught by quality control inspections, an early failure is likely to result. Early failures can be eliminated by a "burn-in" period during which the equipment is operated at stress levels approximating or exceeding the intended actual operating conditions. The equipment is released for actual use only when it has successfully passed through the "burn-in" period, usually by experiencing a specified period of time "failure free."

Chance failures are those failures that result from strictly random or chance causes. They cannot be eliminated by lengthy burn-in periods or by good preventive maintenance practices. When the equipment's specified operating conditions and design levels are exceeded owing to random events, a chance failure could occur.

Wear-out failures occur at the end of the equipment's useful life and are the result of equipment deterioration due to age or use. For example, light bulbs will eventually wear out and fail regardless of how well they are made. The only way to reduce wear-out failures is to replace or repair the deteriorating component before it fails.

Figure 1 illustrates that during the useful life period the failure rate is constant. A constant failure rate is described by the exponential failure distribution. Thus, the exponential failure model reflects the fact that the item must represent a mature design whose failure rate, in general, is primarily comprised of stress-related failures. This means that early failures have been minimized and wear out is not noticeable or is beyond the period of concern.

²R&M Division Directorate for Product Assurance, U.S. Army Aviation Systems Command. Pocket Handbook on Reliability. September 1975, p. 11.

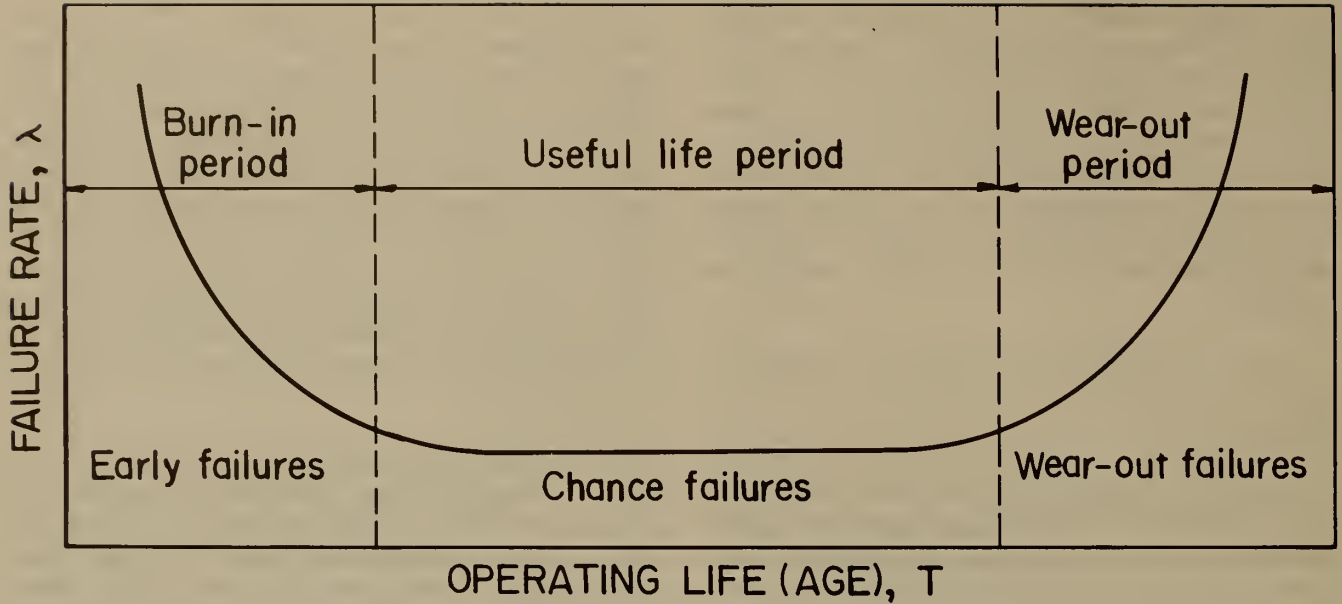


FIGURE 1. - Failure rate as function of equipment age.

The magnitude of this failure rate is directly related to the stress-strength ratio of the item. The exponential model can be derived from the basic notions of probability. When a fixed number, N_o , of components are repeatedly tested, there will be, after a time t , N_s components that survive the test and N_f components that fail. The reliability or probability of survival is at any time t during the test

$$R(t) = \frac{N_s}{N_o} = \frac{N_s}{(N_s + N_f)}$$

Since $N_s = N_o - N_f$, reliability can be written

$$R(t) = \frac{N_o - N_f}{N_o} = 1 - \frac{N_f}{N_o} = 1 - F(t)$$

and

$$\frac{dR}{dt} = \frac{-1}{N_o} \frac{dN_f}{dt} = -f(t)_i$$

where $f(t)_i$ = the failure density function (the probability that a failure will occur in the next time increment dt .)

The hazard rate $z(t)$ is defined as the ratio of the fractional failure rate to the fractional surviving quantity; that is, the number of the original population still operating at time t , or simply the conditional probability of failure.

$$z(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1-F(t)} = \frac{f(t)}{1 - \int_0^t f(t)dt}$$

for the exponential distribution

$$f(t) = \lambda e^{-\lambda t}$$

and

$$z(t) = \lambda.$$

In general, it can be assumed that the hazard rate of electronic elements and systems remains constant over practical intervals of time, and that $z(t)_i = \lambda_i$. Hence, λ_i , a constant, represents the expected number of random failures per unit of operating time of the i^{th} element (the failure rate.) Thus, when a constant failure rate can be assumed

$$z(t)_i = \lambda_i = \frac{f(t)_i}{R(t)_i} = \frac{-dR(t)_i}{R(t)_i dt}$$

Solving this differential equation for $R(t)$, gives the exponential distribution function commonly used in reliability prediction:³

$$R(t)_i = e^{-\lambda_i t},$$

where $R(t)$ = the probability the item will operate without failure for the time period t (usually expressed in hours) under stated conditions,

e = 2.7182...., the base of the natural logarithms,

and λ = the equipment failure rate (usually expressed in failures per hour) and is a constant for any given set of stress, temperature, and quality level conditions. It is determined for parts and components from large-scale data collection and/or test programs.

When appropriate values of λ and t are inserted into the above expression, the probability of success (reliability) is obtained for that time period.

As a specific example, let $\lambda = 0.05$ failure per hour and $t = 1$ hour; then

$$\begin{aligned} R(t) &= e^{-\lambda t} \\ &= e^{-0.05(1)} \\ &= 0.951. \end{aligned}$$

In other words, there is a 95.1-percent chance that the equipment will operate successfully for 1 hour.

The reciprocal of the failure rate λ is defined as the mean time between failures (MTBF):

$$\text{MTBF} = 1/\lambda.$$

The MTBF is primarily a figure of merit by which one hardware item can be compared with another.

To obtain the failure rate and, therefore, the MTBF, a method for estimating part failure rates is needed. The most direct approach involves the use of large-scale data collection efforts to obtain the relationships between engineering and reliability variables and to develop factors for adjusting the reliability to estimate field reliability when considering application conditions.

Failure data obtained from field use of past systems are not always applicable to future concepts. Data obtained on a system used in one environment may not be applicable for a different environment, especially if the new environment substantially exceeds the design capabilities. Thus, a fundamental limitation on reliability prediction is the ability to accumulate data of known validity for the new application.

Once the failure rates for the various components have been established and the MTBF of the system has been determined, it would then be possible to develop a maintenance and repair program to insure high system availability $[A(t)]$. This is the ability of the system under the combined aspects of its reliability and maintenance to perform its required function at a stated instant in time (t). The key factors influencing availability, therefore, are mean time between failures (MTBF) and the mean time to repair the failures (MTTR). This relationship can be expressed as⁴

$$A = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}.$$

³Reliability Analysis Center (Griffiss Air Force Base, N.Y.). Reliability Design Handbook No. RDH376. March 1976, pp. 19-21.

⁴Page 292 of work cited in footnote 3.

For an example, assume the MTBF for a system is 100 hours and that the MTTR is 0.5 hour. The availability of the system then would be

$$A = \frac{100}{100+0.5}$$

$$= 0.995.$$

Therefore, the system would be available to perform its required function 99.5 percent of the time.

Reliability generally differs from availability because reliability requires the continuation of the normal state over the whole interval (0,t); which means,

no failures. However, a component can still contribute to the system availability $A(t)$ if the component failed before time t , is then repaired, and is normal again at time t .⁵

If the hardware failure rates of critical components are unacceptably high, these short-life components can be replaced with more reliable parts. Procedures can also be implemented to provide the necessary spare parts and tools for quickly repairing critical components when they fail. Thus, by increasing the system MTBF and decreasing the MTTR, the equipment will be more readily available to perform its intended functions.

RELIABILITY RESEARCH PROGRAM

A systems approach to the reliability problem has been undertaken by the Bureau of Mines. Studies are being done to look at both the overall performance of the system and the interaction of the various subsystems.

For the hardware subsystem, work is being conducted on developing performance specifications for transducers that will be used in mine-monitoring systems. Also, a test criterion has been developed for the acceptability of mine instrumentation.⁶ This test criterion includes reliability acceptance testing of mine instrumentation developed using the guidelines of Military Standard (MIL-STD)781 (Reliability Design Qualification and Production Acceptance Tests) and will be used to determine if equipment meets the manufacturer's specifications when operated in a mine environment. The appropriate parameters of the mine environment that will affect the instrumentation have also been developed under this effort.

For the software of a computerized mine-monitoring system, there is presently no mechanism for specifying qualities or characteristics, such as reliability, maintainability, or usability. The importance of these software qualities is recognized by the Bureau, and in-house work is currently being done to review the work performed by the military and industry to determine if their approaches to software reliability can be applied to mine-monitoring systems. These approaches basically consist of software reliability models and automated verification systems.

In the area of data transmission, in-house and contract work is being performed to evaluate various aspects of data security and transmission reliability. These studies will help to provide a reliable link between the transducers and the computer processors.

To evaluate systems that are currently being marketed, a methodology

⁵Henley, E. J., and H. Kumamoto. Reliability Engineering and Risk Assessment. Prentice-Hall, Inc., Englewood Cliffs, N.J., 1981, p. 180.

⁶Trelewicz, K. Environmental Test Criteria for the Acceptability of Mine Instrumentation. Dayton T. Brown, Inc., BuMines Contract J0100040, June 1981.

for identifying safety hazards inherent in underground monitoring equipment is being developed. This methodology consists of performing functional analysis, fault tree studies, hazard analysis, and parts count reliability predictions. The information obtained from this methodology will be used to obtain approximate mean time between failure data and to evaluate the hazards associated with the failures that might occur.

Another area of study will include the development of a test criterion and a test fixture for mine-monitoring systems. This test fixture will enable the evaluation of a mine-monitoring system when exposed to various simulated mine conditions and will provide a means of determining system characteristics such as response time and ability to handle multiple-alarm conditions.

An important link between all these areas is a proper data base. Because of the recent emergence of computerized mine-monitoring systems, not much information has been gathered about system reliability or system failure rates and causes during operation in a mine environment. Therefore, the Bureau has initiated several demonstration projects to acquire first-hand information on the operation of these systems. Currently, three mine-monitoring systems are being demonstrated. A minewide evaluation of an intrinsically safe system will be performed at the Lucerne coal mine. At Black River, a limestone mine, a hybrid telemetry-tube bundle system will be evaluated. The Bruceton demonstration, also a hybrid telemetry-tube bundle system, will be evaluated for its air-quality-monitoring capabilities in support of the other projects. Ideas and equipment will be tested here first before installation in the Lucerne and Black River projects.

In-house work will then be performed to set up the necessary data bases to support the current and future Bureau reliability studies. For example, transducer failure rates, calibration

accuracies, data transmission error rates, and hardware and software failure rates and causes will all be evaluated. This information will then be used in developing reliability prediction models and mean-time-between-failure data.

Future areas of study will be devoted to developing reliability design guidelines and specifications for computerized mine-monitoring systems. This effort will enable manufacturers, mine operators, and regulatory agencies to apply proven reliability techniques and procedures to computerized monitoring equipment being used in a mining environment. These in-house projects will be conducted with the support of the Reliability and Compatibility Division of the Rome Air Development Center, Griffiss Air Force Base, N.Y.

The guidelines developed will be generic in part, providing the manufacturers with flexibility in specifying system functional and alternative modes of operation and physical boundaries, such as dimensions, weight, capabilities of materials, and power sources. They will, however, be more specific in areas such as defining the environmental profile, recommended alarm rates, transducer location, and redundancy of coverage, and determining which conditions actually constitute product failures. Then, the guidelines will be definitive in supplying proven reliability models and techniques. These can be applied by the manufacturers to their equipment in all phases of the system's life cycle. The models will include reliability block diagrams, probability equations, part failure modeling, prediction techniques (based on failure rate data obtained from Bureau demonstration projects and mine operators' data), and system modeling concepts pertaining to reliability as it impacts personnel safety, mission success, and unscheduled maintenance.

Finally, a model for developing reliability growth will be established that will account for detecting and analyzing hardware and software failures, feedback

and redesign of problem areas, implementation of corrective actions, and retesting.

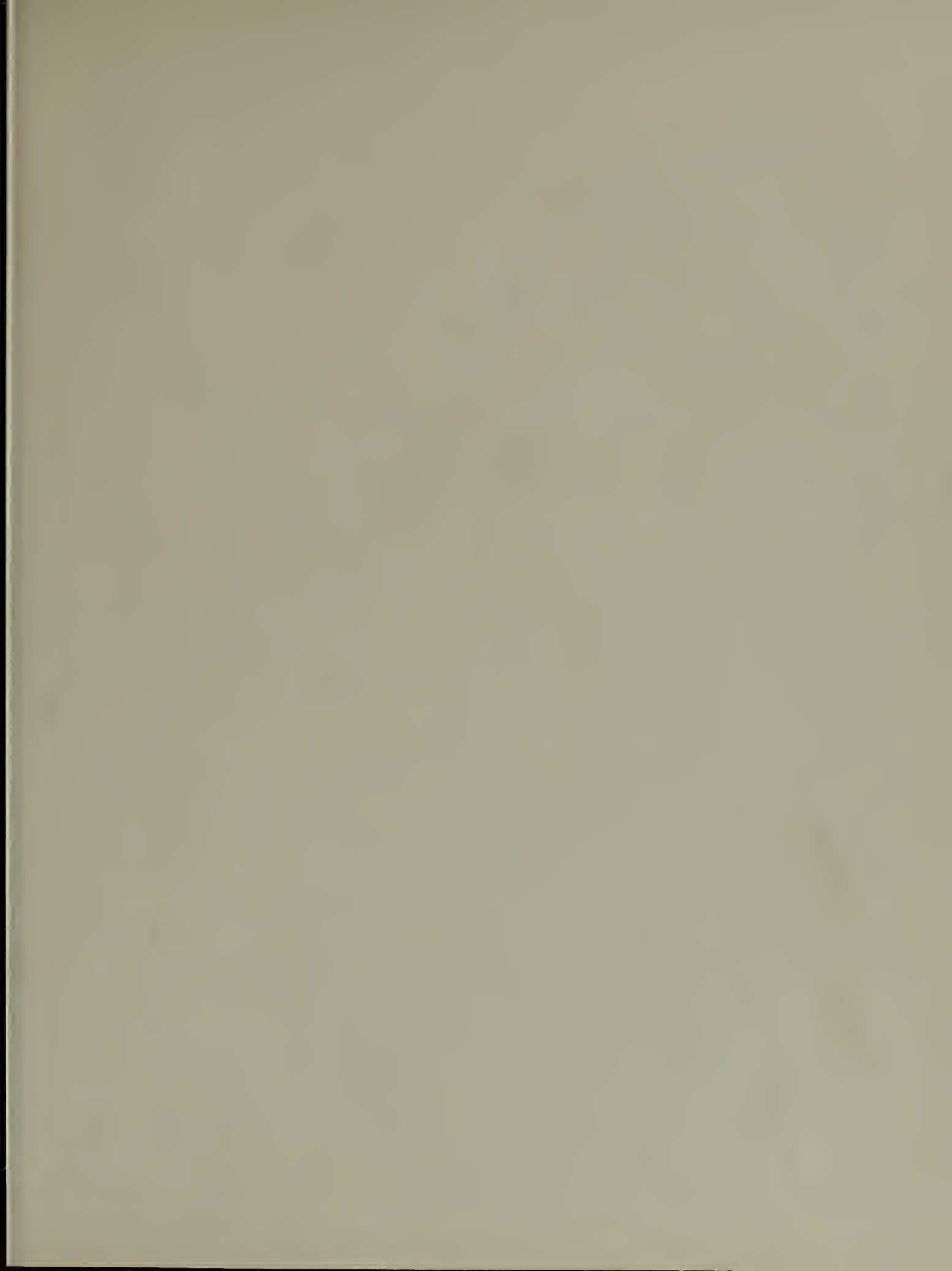
Therefore, to provide an effective design program, the Bureau must develop

reliability models that account for all of the system's life cycle factors and the environmental conditions to be encountered, and also provide for proper maintenance and feedback systems to insure reliability.

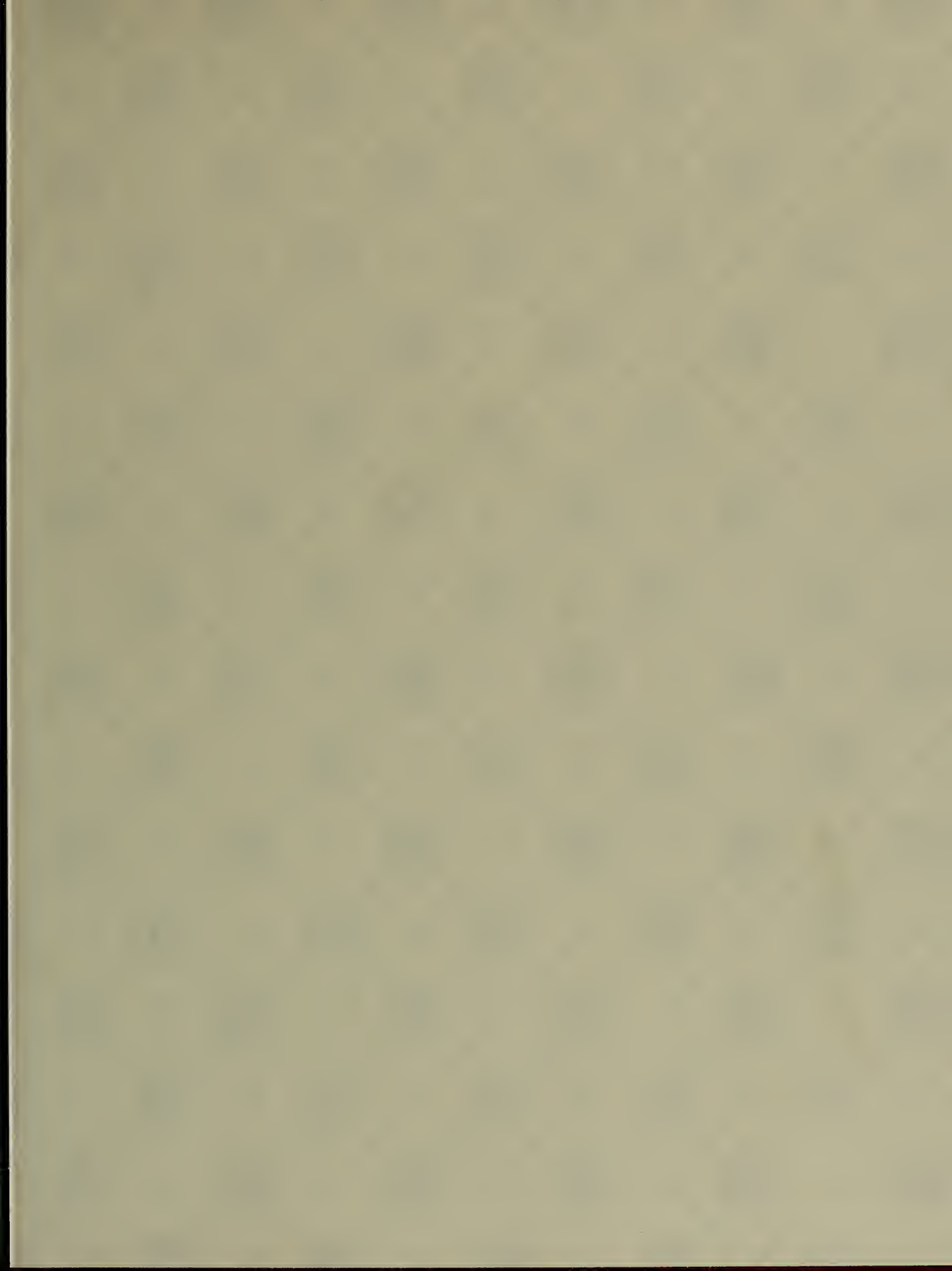
CONCLUSION

Computerized mine-monitoring systems can be used to fill existing gaps in environmental monitoring methods and to provide enhanced production monitoring. However, for a computerized system to be accepted by the mining industry, it has to be demonstrated that such a system

would be reliable and would provide an advantage over current monitoring methods in safety and/or cost. It is the Bureau's intention to provide the proper data bases and guidelines to assure the mining industry that computerized mine-monitoring systems can be relied upon.











WERT
BOOKBINDING
MIDDLETOWN, PA.
SEPT. 82
We're Quality Bound

LIBRARY OF CONGRESS



0 002 959 817 4